# Cerner
## Application Service Provider Privacy & Security Policies

| | |
|---|---|
| **Access** | Access to a person's health record in Cerner solutions is controlled via a multi-level role-based security model. No user may access any patient's record without first declaring a reason for the access or relationship to the patient. If the user does not have a relationship with the patient, the system opens the Assign Relationship dialog box, requesting the user to select a relationship with that patient. The relationships displayed are based on the relationships chosen for the user's position by your organization. Those relationships include both visit-specific and lifetime relationships. |
| **Authorization** | Authenticated user names and passwords are presented to the client specified domain that determines whether the username is authorized. This authorization will allow you to access the application and the specific functions based on your permissions. Users are authorized to perform tasks in the system application based upon the group and role assignment associated to each user in your organization. |
| **Authentication** | There are two levels of authentication: Citrix and Active Directory. Both check for user authentication against the existing repository. Additionally, two pieces of information are necessary at the time of user login, the username and password. (You can define a default domain; otherwise you will also enter a domain). The system locates the security server in the domain specified and determines whether the username is valid. If the username is located and is valid, the server creates a token containing a ticket encrypted with the username's password. The server returns this token to the PC. The password entered by you is then used to decrypt the token. If you entered an incorrect password the token cannot be opened, an error message is displayed and an unsuccessful attempt is logged. If you entered a correct password authentication is successful and you are allowed to use your token to attempt access to the application and its servers via the authorization process. |
| **Audit** | Cerner supports an audit logging solution that supports recording end user operations to patient information that create, modify, verify, error correct, print, or inquire into the patient record. The audit logging also includes recording of definition and management of key relationships in the security profile of end users, including association of users to positions or organizations, positions to relationship types, positions to application groups, and application tasks to application groups. |
| **Secondary Uses of Data** | Data is housed at the state of the art data center. Cerner does not use client data for any secondary uses. |
| **Data Ownership** | Client maintains ownership of data. Upon contract termination Cerner will provide your data on an electronic media. Discrete data will be in .csv format (you can read this with Excel). Attachments will be provided to the clients as images on a CD. Additional fees may apply for custom exports. |